be encrypted by the content key K_{co}. The ID of a content provider indicates an ID of a content provider 2 that encrypts album contents.

The version of a key indicates revision information of a key (a content key K_{co}) revised according to a usage period. The signature is attached to the entirety from the type of data to the public key certificate excluding the signature from data of the single contents. An algorithm and a parameter used in preparing the signature as well as a key to be used for verification of the signature are included in the public key certificate.

In addition, in key data for album contents, with the addition of a signature to the entire album contents, tamper or the like can be checked for key data of each single content as well together with key data of the album contents simply by verifying the signature without respectively verifying key data for a plurality of single contents stored in key data for the album contents, hence, the verification of a signature can be thereby simplified.

Figure 51 illustrates operations of mutual authentication of an encryption processing section 65 and an extension section 66, in which one common key uses DES that is a common key encryption. In Figure 51, given that A is an extension section 66 and B is an encryption processing section 65, the encryption processing section 65 generates a random number R_B of 64 bits, and transmits R_B and ID_B that is its own ID to the extension section 66 via an upper controller 62. The extension section 66 having received the transmission generates a random number R_A anew, encrypts R_A, R_B and ID_B using a key K_{AB} in a CBC mode of DES,